NIKANDER
Serial No. 10/091,288

Atty Dkt: 3772-8
Art Unit: 2142

AMENDMENTS TO THE DRAWINGS:

Please replace original Fig. 1 with the attached Replacement Sheet for Fig. 1.

NIKANDER
Serial No. 10/091,288

Atty Dkt: 3772-8
Art Unit: 2142

REMARKS/ARGUMENTS

Reexamination of the captioned application is respectfully requested.

A. SUMMARY OF THIS AMENDMENT

By the current amendment, Applicant basically:

1. Editorially amends the specification.
2. Amends claims 7 and 17.
3. Amends Fig. 1 in the manner shown in the attached Replacement Sheet.
4. Respectfully traverse all prior art rejections.

B. AMENDMENTS TO THE DRAWINGS

The attached Replacement Sheet for Fig. 1 includes amendments such as labeling symbol 5 as "Internet"; symbol 6 as "foreign agent (access node)"; and supplying reference numerals 4, 8, and 9 in a manner understood from the last full paragraph of page 9 as well as the paragraph bridging pages 9 and 10 of the specification.

C. SELECTED COMMENTS REGARDING THE DISCLOSURE

As explained in Applicants' specification, the IPv6 protocol allows client terminals themselves to generate the interface Identifier part of an IP address which is subsequently combined with a routing prefix to generate the full IPv6 address. However, the IPv6 protocol's generation of the interface Identifier part of an IP address can result in an address conflict. The IPv6 protocol makes an effort to prevent address conflicts within a local area in the following manner: once a terminal has generated a new IP address it must broadcast this address over the local area. If another terminal already possesses the same address that terminal will generate a response. The originating terminal must then generate an alternative address, and the process is repeated until such time as the terminal arrives at an IP address which does not result in any conflict.

The problem with the aforedescribed duplicate address detection procedure is that, unless some security mechanism is put in place, it provides an opportunity for malicious third parties to launch Denial of Service attacks. More particularly, when a malicious terminal receives an IP address advertisement message, it can always reply claiming ownership of the address. The originating terminal may never be able to obtain a useable IP address.

Applicant provides a mechanism which, in the event of an alleged conflict, is able to resolve the conflict in favor of the true owner of the IP address. This mechanism is achieved by a controlling node within the network requesting (from each party claiming to own an IP address) a token or "component" which the true address owner will already have in his possession, but which a malicious party cannot easily and quickly generate. This component effectively provides a seed value from which the Interface Identifier part of the IP address is generated by the application of a one-way coding function. The use of a one-way coding function means that a malicious party cannot reverse the operation, i.e. generate the component from the Interface Identifier part. Importantly, Applicant's address ownership mechanism does not need or rely upon a shared secret between any of the parties. It is only necessary that all parties have access to the published one-way coding function.

D. PATENTABILITY OF THE CLAIMS

Claim 1 stands rejected under 35 USC 103(a) as being over U.S. Patent 5,351,295 to Perlman et al. Claims 1-11 stand rejected under 35 USC §103(a) as being unpatentable over U.S. Patent 5,351,295 to Perlman et al in view of Internet Draft by Narten. Claims 17-18 stand rejected under 35 USC §102(b) as being anticipated by U.S. Patent 5,872,917 to Hellman. Claims 19-20 stand rejected under 35 USC §103(e) as being unpatentable over U.S. Patent 5,872,917 to Hellman in view of Internet Draft by Narten. All prior art rejections are respectfully traversed for at least the following reasons.

Perlman describes a mechanism whereby members of a group can securely exchange network addresses with one another. The process relies upon all of the group members having access to a shared secret. Penman does not describe a method of verifying that a host coupled to an IP network is actually authorized to use an IP address which the host claims to own. According to Perlman, a host which is a member of the group can select any network address and the receiving hosts will implicitly assume that the sending host owns the address on the basis of a shared secret. Of course, there is nothing to prevent one of the group members from claiming to own an IP address which actually belongs to a host which is not one of the group members. Perlman does not describe any mechanism for addressing such conflicts.

Nor does Ford teach any means for overcoming this deficiency of Perlman. Ford is only concerned with providing a mechanism for generating IP addresses at client terminals. According to Ford, conflicts are overcome using the (IPv6 type) advertisement and response procedure described above. Ford is, therefore, only concerned with accidental conflicts, and does not present any mechanism which would overcome the denial of service attacks which can be made by malicious parties.

The teaching of Narten is essentially the same as Ford, i.e., the use of a hash function to generate the Interface Identifier part of an IP address. Perlman teaches a method of securely exchanging addresses between group members which is based upon a shared secret. It does not teach a method of proving ownership of these addresses. Narten does not address this deficiency.

U.S. Patent 5,872,917 to Hellman does not provide a basis for denying patentability to any of applicant's claims. Please keep in mind that claim 17 incorporates the limitations of independent claim 1, and thus is more than a challenge, response, verification scenario.

The deficiencies of U.S. Patent 5,872,917 to Hellman are very similar to those of Perlman. Hellman relies upon all the authenticating party and/or the party to be authenticated proving that they know a shared password (*see*, e.g., col. 3, lines 33 – 35). Nor does Hellman describe a method of verifying that a host coupled to an IP network is actually authorized to use an IP address which the host claims to own. Rather, Hellman's interaction involves an exchange of our values: the user's ID; the host's challenge; the user's response; and the host's response (*see*, e.g., col. 6, lines 23 - 28). The user's response to the host's challenge is generated from the shared secret password, the host's challenge, and an extra value PAD using a function FA. The authentication transaction is not based on application of a one-way coding function to a component supplied by the user, and certainly does not involve a comparison of a result or derivative of the function application result against an interface identifier part of an IP address.

E. MISCELLANEOUS

In view of the foregoing and other considerations, all claims are deemed in condition for allowance. A formal indication of allowability is earnestly solicited.

The Commissioner is authorized to charge the undersigned's deposit account #14-1140 in whatever amount is necessary for entry of these papers and the continued pendency of the captioned application.

Should the Examiner feel that an interview with the undersigned would facilitate allowance of this application, the Examiner is encouraged to contact the undersigned.

NIKANDER
Serial No. 10/091,288

Atty Dkt: 3772-8
Art Unit: 2142

Respectfully submitted,
NIXON & VANDERHYE P.C.

By: _____
H. Warren Burnam, Jr.
Reg. No. 29,366

HWB:lsh
1100 North Glebe Road, 8th Floor
Arlington, VA 22201-4714
Telephone: (703) 816-4000
Facsimile: (703) 816-4100
Attachments:
Replacement Sheet for Fig. 1